

1 Bevin Allen Pike (SBN 221936)  
Bevin.Pike@capstonelawyers.com  
2 Robert K. Friedl (SBN 134947)  
Robert.Friedl@capstonelawyers.com  
3 Trisha K. Monesi (SBN 303512)  
Trisha.Monesi@capstonelawyers.com  
4 Capstone Law APC  
1875 Century Park East, Suite 1000  
5 Los Angeles, California 90067  
Telephone: (310) 556-4811  
6 Facsimile: (310) 943-0396

7  
8 Attorneys for Plaintiffs  
Susan Webber and Livia Soibelman

9 UNITED STATES DISTRICT COURT  
10 NORTHERN DISTRICT OF CALIFORNIA

11 SUSAN WEBBER and LIVIA  
12 SOIBELMAN, individually, and on behalf  
13 of a class of similarly situated individuals,

14 Plaintiffs,

15 v.

16 UBER TECHNOLOGIES, INC., a  
Delaware corporation; RASIER-CA, LLC,  
17 a Delaware limited liability company; and  
RASIER, LLC, a Delaware limited  
18 liability company,

19 Defendants.

Case No.:

**CLASS ACTION COMPLAINT FOR:**

- (1) Negligence
- (2) Violations of Unfair Competition Law,  
California Business & Professions Code  
§ 17200 *et seq.*
- (3) Violations of California's Customer  
Records Act, California Civil Code §  
1798.80 *et seq.*

**DEMAND FOR JURY TRIAL**

## INTRODUCTION

1. Plaintiffs Susan Webber and Livia Soibelman (“Plaintiffs”) bring this action for themselves and on behalf of all persons who reside in the United States and who created an account with Uber Technologies, Inc., Rasier-CA, LLC, and Rasier, LLC (“Defendants” or “Uber”) as a driver (“Uber Drivers”) or a rider (“Uber Riders”) that was vulnerable or potentially vulnerable to cybersecurity breaches (“Uber Users”).

2. Uber requires its Users to provide personally identifiable information (“PII”) upon registering as a driver or rider via Defendants’ website or mobile phone application and Users expect Defendants to maintain strict confidentiality of the PII in Uber’s possession. Throughout the course of its business, Uber has collected and maintained an extensive amount of its Users’ personal information including, without limitation, Users’ names, email addresses, telephone numbers, dates of birth, credit card numbers, bank account numbers, Social Security Numbers, driver’s license numbers and trip location history. However, on information and belief, Defendants failed, and continues to fail, to provide adequate protection of its Drivers’ and Riders’ personal and confidential information and has egregiously failed to provide sufficient and timely notice or warning of potential and actual cybersecurity breaches to its users.

3. In an ongoing investigation, Uber recently revealed that its Users’ personal information was subject to a massive data security breach in late 2016, **affecting approximately 600,000 Uber Drivers’ and 57 million Uber Riders’ PII** (“2016 Breach”). Uber released a statement on November 21, 2017, publicly exposing details of the 2016 data breach for the first time. According to the statement, Defendants learned of the data breach as early as “late 2016” yet failed to inform or notify Uber Users that their PII may be compromised as a result of the breach. Rather, on information and belief, Uber chose to negotiate directly with the cyber attackers to actively conceal the data breach from Users and compensate the attackers for “assurances” that Uber Users’ stolen PII had been destroyed.<sup>1</sup>

---

<sup>1</sup> Dara Khosrowshahi, CEO of Uber Technologies, Inc., stated that “[I]n late 2016[,] we became aware that two individuals outside the company had inappropriately accessed user

4. As a result of Defendants' failure to maintain adequate security measures and timely security breach notifications, Uber Users' personal and private information has been repeatedly compromised and remains vulnerable. In fact, according to Uber, it has just begun to contact those Users currently known to have compromised and stolen PII, *over a year after Uber learned of the breach*. Further, Uber Users have suffered an ascertainable loss in that they must undertake additional security measures, some at their own expense, to minimize the risk of future data breaches including, without limitation, changing driver's license numbers, credit card numbers, bank account numbers and related passwords, and purchasing a security freeze on their credit files. However, due to Uber's ongoing and incomplete investigation, Uber Users have no guarantee that the above security measures will in fact adequately protect their personal information. As such, Plaintiffs and other Class Members have an ongoing interest in ensuring that their personal information is protected from past and future cybersecurity threats.

#### THE PARTIES

5. Plaintiff Susan Webber ("Plaintiff Webber") is a citizen of the state of California, residing in San Diego, California. Plaintiff Webber has worked as an Uber Driver since approximately June 2016 and provided Defendants with PII including her name, email address, telephone number, mailing address, Social Security Number, bank account number, driver's license number, and date of birth. As of the date of filing of this complaint, Plaintiff Webber has not been notified by Uber regarding the data breach but has taken steps to secure her PII after learning of the breach through public news sources, including changing her Uber account password.

6. Plaintiff Livia Soibelman ("Plaintiff Soibelman") is a citizen of the state of California, residing in Redondo Beach, California. Plaintiff Soibelman has been an Uber

---

data stored on a third-party cloud-based service that we use. [...] [T]he individuals were able to download files containing a significant amount of other information, including: The names and driver's license numbers of around 600,000 drivers in the United States; Some personal information of 57 million Uber users around the world, including the drivers described above. This information included names, email addresses and mobile phone numbers." *Available at* <https://www.uber.com/newsroom/2016-data-incident> (last visited Nov. 22, 2017).

1 Rider since approximately 2013 and has provided Uber with PII including her name, email  
2 address, telephone number, mailing address, billing address, and credit card numbers. As of  
3 the date of filing of this complaint, Plaintiff Soibelman has not been notified by Uber  
4 regarding the data breach but has taken steps to secure her PII after learning of the breach  
5 through public news sources, including changing her Uber account password.

6 7. Defendant Uber Technologies, Inc. (“Uber”) is a corporation organized and in  
7 existence under the laws of the State of Delaware and registered to do business in the State of  
8 California. Uber Technologies, Inc. Corporate Headquarters are located at 1455 Market  
9 Street, 4th Floor, San Francisco, California.

10 8. Defendant Rasier-CA, LLC is a limited liability corporation organized and in  
11 existence under the laws of the State of Delaware and registered to do business in the State of  
12 California. On information and belief, Rasier-CA, LLC is a wholly-owned subsidiary of Uber  
13 Technologies, Inc. Rasier-CA, LLC’s Corporate Headquarters are located at 1455 Market  
14 Street, 4th Floor, San Francisco, California.

15 9. Defendant Rasier, LLC is a limited liability corporation organized and in  
16 existence under the laws of the State of Delaware and registered to do business in the State of  
17 California. On information and belief, Rasier, LLC is a wholly-owned subsidiary of Uber  
18 Technologies, Inc. Rasier, LLC’s Corporate Headquarters are located at 1455 Market Street,  
19 4th Floor, San Francisco, California.

20 10. At all relevant times, Defendants were and are engaged in the business of  
21 providing and arranging ride-share services via its mobile application and website in San  
22 Francisco County and throughout the United States of America.

### 23 JURISDICTION

24 11. This is a class action.

25 12. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C.  
26 § 1331 because this action arises under the Constitution or laws of the United States and the  
27 Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) and (6), in that, as to each Class defined  
28 herein:

- 1 (a) the matter in controversy exceeds \$5,000,000.00, exclusive of interest  
2 and costs;
- 3 (b) this is a class action involving 100 or more class members; and
- 4 (c) this is a class action in which at least one member of the Plaintiffs' class  
5 is a citizen of a State different from at least one Defendant.

6 13. The Court has personal jurisdiction over Defendants, which have at least  
7 minimum contacts with the State of California because their headquarters are located there  
8 and they have conducted business there and have availed themselves of California's markets  
9 through their ride-sharing services.

#### 10 **VENUE**

11 14. Uber, through its ride-sharing business has established sufficient contacts in  
12 this district such that personal jurisdiction is appropriate. Defendant is deemed to reside in  
13 this district pursuant to 28 U.S.C. § 1391(a).

14 15. In addition, all Defendants are headquartered in San Francisco, have conducted  
15 business in this district, and have availed themselves of California's markets through their  
16 marketing, sale, and administration of ride-sharing services. Venue is proper in this Court  
17 pursuant to 28 U.S.C. § 1391(a).

#### 18 **FACTUAL ALLEGATIONS**

19 16. To utilize Uber's ride-share services, Drivers and Riders, including Plaintiffs  
20 and other Class Members, must create an account operated by Defendants. On information  
21 and belief, Uber controls and operates the mobile application software that requests and stores  
22 Uber Rider information and Rasier, LLC controls and operates the mobile application  
23 software that requests and stores Uber Driver information.<sup>2</sup> As such, Defendants have  
24 collected and maintained an extensive amount of Uber Users' personal information including,  
25 without limitation, Users' names, email addresses, telephone numbers, dates of birth, credit  
26

27 <sup>2</sup> See Technology Services Agreement, Dec. 11, 2015, *available at*  
28 <https://assets.documentcloud.org/documents/2645988/RASIER-Technology-Services-Agreement-Decmeber-10.pdf> (last visited Nov. 22, 2017).

card numbers, bank account numbers, Social Security Numbers, driver's license numbers and trip location history. Drivers and Riders provide this personal information to Uber in reliance on Defendants' assurances as to the protection and security of its Users' PII.

17. However, Defendants have failed, and continue to fail, to provide adequate protection of the Uber Drivers' and Riders' personal and confidential information and have egregiously failed to provide sufficient and timely notice or warning of potential and actual cybersecurity breaches to Uber Users.

18. In an ongoing investigation, Uber recently revealed that its Users' personal information was subject to a massive data security breach in late 2016, affecting approximately 600,000 Uber Drivers' and 57 million Uber Riders' PII. Uber released a statement on November 21, 2017, publicly exposing details of the 2016 data breach for the first time to its Users. According to the statement, Uber learned of the data breach as early as "late 2016" yet failed to inform or notify Uber Users that their PII may be compromised as a result of the breach. Rather, on information and belief, Uber chose to negotiate directly with the cyber attackers to actively conceal the data breach from Users and compensate the attackers for "assurances" that Uber Users' stolen PII had been destroyed. Uber's November 21, 2017, statement revealed the following:

As Uber's CEO, it's my job to set our course for the future, which begins with building a company that every Uber employee, partner and customer can be proud of. For that to happen, we have to be honest and transparent as we work to repair our past mistakes.

I recently learned that in late 2016 we became aware that two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use. The incident did not breach our corporate systems or infrastructure.

Our outside forensics experts have not seen any indication that trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded. However, the individuals were able to download files containing a significant amount of other information, including:

- The names and driver's license numbers of around 600,000 drivers in the United States. Drivers can learn more here.
- Some personal information of 57 million Uber users around the world, including the drivers described above. This information included names, email addresses and mobile phone numbers. Riders can learn more here.

At the time of the incident, we took immediate steps to secure the data and shut down further unauthorized access by the individuals. We subsequently identified

the individuals and obtained assurances that the downloaded data had been destroyed. We also implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts.

You may be asking why we are just talking about this now, a year later. I had the same question, so I immediately asked for a thorough investigation of what happened and how we handled it. What I learned, particularly around our failure to notify affected individuals or regulators last year, has prompted me to take several actions:

- I've asked Matt Olsen, a co-founder of a cybersecurity consulting firm and former general counsel of the National Security Agency and director of the National Counterterrorism Center, to help me think through how best to guide and structure our security teams and processes going forward. Effective today, two of the individuals who led the response to this incident are no longer with the company.
- We are individually notifying the drivers whose driver's license numbers were downloaded.
- We are providing these drivers with free credit monitoring and identity theft protection.
- We are notifying regulatory authorities.
- While we have not seen evidence of fraud or misuse tied to the incident, we are monitoring the affected accounts and have flagged them for additional fraud protection.

None of this should have happened, and I will not make excuses for it. While I can't erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes. We are changing the way we do business, putting integrity at the core of every decision we make and working hard to earn the trust of our customers.<sup>3</sup>

19. As a result of Defendants' failure to maintain adequate security measures and timely security breach notifications, Uber Users' personal and private information has been repeatedly compromised and remains vulnerable. In fact, according to Uber, it has just begun to contact those Users currently known to have compromised and stolen PII, over a year after Defendants learned of the breach. Further, Uber Users have suffered an ascertainable loss in that they must undertake additional security measures, some at their own expense, to minimize the risk of future data breaches including, without limitation, changing driver's license numbers, credit card numbers, bank account numbers and related passwords, and purchasing a security freeze on their credit files. However, due to Defendants ongoing and incomplete investigation, Uber Users have no guarantee that the above security measures will in fact

<sup>3</sup> Available at <https://www.uber.com/newsroom/2016-data-incident> (last visited Nov. 22, 2017).

adequately protect their personal information. As such, Plaintiffs and other Class Members have an ongoing interest in ensuring that their personal information is protected from past and future cybersecurity threats

20. The insufficient security policies and procedures implemented by Defendants is a material fact that a reasonable consumer would consider when deciding whether to create an account and provide Defendants with personal and confidential information. Had Plaintiffs and other Class Members known that Defendants failed to employ necessary and adequate protection of their personal information, they would not have created an Uber Driver or Rider account. In fact, Plaintiffs and other Class Members relied on Uber's Privacy policies ensuring implementation of "physical, electronic, and procedural safeguards" to protect their personal information.

### CLASS ACTION ALLEGATIONS

21. Plaintiffs bring this lawsuit as a class action on behalf of themselves and all others similarly situated as members of the proposed Class pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

22. The Class is defined as:

**Nationwide Class:** All individuals residing in the United States who registered for an account as an Uber Driver and/or Uber Rider, at any time, from four years prior to the filing of this complaint to the time of class certification, with Uber whose personal or financial information was accessed, compromised, or stolen from Defendants in the 2016 Breach (the "Nationwide Class" or "Class").

**California Rider Sub-Class:** All members of the Nationwide Class who registered for an account as an Uber Rider and reside in the State of California.

23. Collectively, the Nationwide Class and the California Rider Sub-Class, and their class members, will be referred to herein as the "Class" and "Class Members," except where otherwise noted.

24. Excluded from the Class are: (1) Defendants, any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; (3) any Judge sitting in the presiding state and/or federal court system who may hear an appeal of any judgment entered; and (4) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiffs reserve the right to amend the Class and Sub-Class definition if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

25. Numerosity: Although the exact number of Class Members is uncertain and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable. The disposition of the claims of these Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control.

26. Typicality: Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class Members, have maintained an Uber account throughout the duration of the class period. The representative Plaintiffs, like all Class Members, have been damaged by Defendants' misconduct in that they have had to undertake additional security measures, at their own expense, to minimize the risk of future data breaches. Furthermore, the factual bases of Defendants' misconduct are common to all Class Members and represent a common thread resulting in injury to all Class Members.

27. Commonality: There are numerous questions of law and fact common to Plaintiffs and the Class that predominate over any question affecting only individual Class Members. These common legal and factual issues include the following:

- (a) Whether Defendants owed a duty of care to Plaintiffs and Class Members with respect to the security of their personal information;
- (b) Whether Defendants had a legal and/or contractual duty to use reasonable security measures to protect Plaintiffs' and Class Members'

personal information;

(c) Whether Defendants took reasonable steps and measures to safeguard Plaintiffs' and Class Members' personal information;

(d) Whether Defendants breached its duty to exercise reasonable care in handling Plaintiffs' and Class Members' personal information;

(e) Whether Defendants acts and omissions described herein give rise to a claim of negligence;

(f) Whether Defendants security procedures and practices violated *California Business & Professions Code* §§ 17200 *et seq.*;

(g) Whether Defendants security procedures and practices violated *California Civil Code* §§ 1798.90 *et seq.*;

(h) Whether Defendants knew or should have known of the 2016 Breach;

(i) Whether Defendants had a duty to promptly notify Class Members that their personal information was, or potentially could be, compromised; and

(j) Whether Plaintiffs and other Class Members are entitled to damages or equitable relief, including but not limited to, a preliminary and/or permanent injunction.

28. Adequate Representation: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs have retained attorneys experienced in the prosecution of complex class actions, including consumer and product defect class actions, and Plaintiffs intend to prosecute this action vigorously.

29. Predominance and Superiority: Plaintiffs and Class Members have all suffered and will continue to suffer harm and damages as a result of Defendants' unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Because of the relatively small size of the individual Class

Members' claims, it is likely that only a few Class Members could afford to seek legal redress for Defendants' misconduct. Absent a class action, Class Members will continue to incur damages, and Defendants' misconduct will continue without remedy. Class treatment of common questions of law and fact would also be a superior method to multiple individual actions or piecemeal litigation in that class treatment will conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

### **FIRST CAUSE OF ACTION**

#### **(Negligence)**

30. Plaintiffs incorporate by reference the allegations contained in each and every paragraph of this Complaint.

31. Plaintiffs bring this cause of action on behalf of themselves and on behalf of the Nationwide Class.

32. Defendants owed a duty to Plaintiffs and Class Member to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal information in their possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, implementing, maintaining and testing Defendants' security systems and protocols, consistent with industry standards and requirements, to ensure that Plaintiffs' and Class Members' personal information in Defendants' possession was adequately secured and protected. Defendants further owed a duty to Plaintiffs and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

33. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate security practices. Defendants solicited, gathered, and stored the personal data provided by Plaintiffs and Class Members in the regular course of its business. Defendants knew that a breach of their systems would cause damages to Plaintiffs and Class Members, and Defendants had a duty to adequately protect such sensitive personal information.

1           34.     Similarly, Defendants owed a duty to Plaintiffs and Class Members to timely  
2 disclose any incidents of data breaches, where such breaches compromised the personal  
3 information of Plaintiffs and Class Members. Plaintiffs and Class Members were foreseeable  
4 and probable victims of any inadequate notice practices. Defendants knew that, through its  
5 actions and omissions, it had caused the sensitive personal information of Plaintiffs and Class  
6 Members to be compromised and accessed by unauthorized third parties yet failed to mitigate  
7 potential harm to Uber Users by providing timely notice of the security breach.

8           35.     Defendants breached the duties owed to Plaintiffs and Class Members by  
9 failing to exercise reasonable care in the adoption, implementation, and maintenance of  
10 adequate security procedures and protocols and by failing to timely notify Plaintiffs and Class  
11 Members of potential and actual security breaches. Defendants' breach of the duties owed to  
12 Plaintiffs and Class Members caused injuries to Plaintiffs and Class Members, including but  
13 not limited to a) theft of their personal information; b) costs associated with the detection and  
14 prevention of identity theft; c) costs associated with time spent and the loss of productivity  
15 from taking time to address and attempt to ameliorate and mitigate the actual and future  
16 consequences of the aforementioned data breaches, including without limitation finding  
17 fraudulent charges, cancelling and reissuing credit cards and bank accounts, purchasing credit  
18 monitoring and identity theft protection, and the stress, nuisance and annoyance of dealing  
19 with all issues resulting from the data breaches; d) the imminent and impending injury flowing  
20 from potential fraud and identity theft posed by the unauthorized control and use of their  
21 personal information by third parties; e) damages to and diminution in value of their personal  
22 information entrusted to Defendants with the understanding that Defendants would safeguard  
23 their data against theft and not allow access and misuse of their data by others; and f) the  
24 continued risk to their personal information, which remains in Defendants' and which is  
25 subject to further breaches so long as Defendants fail to undertake appropriate and adequate  
26 measures to protect data in their possession.

27           36.     But for Defendants' negligent and wrongful breach of the duties owed to  
28 Plaintiffs and Class Members, Plaintiffs and Class Members would not have been harmed and

1 could have taken remedial measures to protect their personal information.

2 37. Plaintiffs and Class Members are entitled to and seek actual damages and  
3 reasonable attorneys' fees and costs.

4 **SECOND CAUSE OF ACTION**

5 **(Violation of California Business & Professions Code § 17200, *et seq.*)**

6 38. Plaintiffs incorporate by reference the allegations contained in each and every  
7 paragraph of this Complaint.

8 39. Plaintiffs bring this cause of action on behalf of themselves and on behalf of the  
9 Nationwide Class, or in the alternative, on behalf of the California Sub-Class.

10 40. As a result of their reliance on Defendants' omissions, Uber Users utilizing its  
11 ride-sharing services suffered an ascertainable loss due to Defendants' failure to provide  
12 adequate protection of its Uber Users' personal and confidential information and failure to  
13 provide sufficient and timely notice or warning of potential and actual cybersecurity breaches.

14 41. California Business & Professions Code § 17200 prohibits acts of "unfair  
15 competition," including any "unlawful, unfair or fraudulent business act or practice" and  
16 "unfair, deceptive, untrue or misleading advertising."

17 42. Plaintiffs and Class Members are reasonable consumers who expected  
18 Defendants to vehemently protect the personal information entrusted to them and to be  
19 informed by Defendants of potential and actual cybersecurity vulnerabilities as soon as  
20 Defendants became aware of such threat.

21 43. Defendants' acts and omissions were intended to induce Plaintiffs and Class  
22 Members' reliance on Defendants' explicit and implied guarantee that their personal  
23 information was secure and protected, to increase the number of Uber Users, and, ultimately,  
24 to increase Defendants' revenues. Plaintiffs and the Class Members were deceived by  
25 Defendants' failure to properly implement adequate, commercially reasonable security  
26 measures to protect their personal information, and Defendants' failure to promptly notify  
27 them of the security breach. As a result, Defendants' conduct constitutes "fraudulent"  
28 business acts or practices.

1           44. Defendants' conduct was and is likely to deceive consumers.

2           45. In failing to implement adequate security procedures and protocols to protect  
3 Plaintiffs and Class Members' personal information and promptly notify Plaintiffs and Class  
4 Members of potential and actual security threats, Defendants have knowingly and  
5 intentionally concealed material facts and breached its duty not to do so.

6           46. Defendants were under a duty to Plaintiffs and Class Members to protect Uber  
7 Users' personal information and promptly notify Uber Users of potential and actual security  
8 threats, and other omitted facts alleged herein, because:

9                   (a) Defendants were in superior positions to know the specifics of a  
10 potential or actual security breach; and

11                   (b) Defendants actively concealed information known to them regarding  
12 potential and actual security breaches affecting Uber Users account  
13 information.

14           47. The facts Defendants concealed from or did not disclose to Plaintiffs and Class  
15 Members are material in that a reasonable person would have considered them to be important  
16 in deciding whether to utilize Defendants' services or cancel, change or otherwise modify  
17 their account information. Had Plaintiffs and other Class Members known that Defendants  
18 failed to employ necessary and adequate protection of their personal information and would  
19 fail to timely notify them of potential security breaches, they would not have created an Uber  
20 Driver or Uber Rider account.

21           48. By their conduct, Defendants have engaged in unfair competition and unlawful,  
22 unfair and fraudulent business practices. Defendants' unfair or deceptive acts or practices  
23 occurred repeatedly in Defendants' trade or business, and were capable of deceiving a  
24 substantial portion of the purchasing public.

25           49. As a direct and proximate result of Defendants' unlawful, unfair and deceptive  
26 practices, Plaintiffs and Class Members will continue to suffer actual damages.

27           50. Defendants have been unjustly enriched and should be required to make  
28 restitution to Plaintiffs and Class Members pursuant to §§ 17203 and 17204 of the California

Business & Professions Code.

**THIRD CAUSE OF ACTION**

**(Violation of the California Customer Records Act,**

**California Civil Code § 1798.80, *et seq.*)**

51. Plaintiffs incorporate by reference the allegations contained in each and every paragraph of this Complaint.

52. Plaintiff Soibelman brings this cause of action on behalf of herself and on behalf of the California Rider Sub-Class.

53. The California Legislature enacted Civil Code § 1798.81.5 “to ensure that personal information about California residents is protected.” The statute requires that any business that “owns, licenses, or maintains personal information about a California resident ... implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

54. Defendants are “business[es]” as defined by Civil Code § 1798.80(a).

55. Plaintiffs and California Rider Sub-Class Members are “individual[s]” as defined by Civil Code § 1798.80(d).

56. The personal information taken in the data breach was “personal information” as defined by Civil Code § 1798.80(e) and 1798.81.5(d), which includes “information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.”

57. The breach of the personal information of “57 million Uber users” was a “breach of the security system” of Defendants as defined by Civil Code § 1798.82(g).

58. By failing to implement reasonable security measures appropriate to the nature

1 of the personal information of Uber Riders, Defendants violated Civil Code § 1798.81.5.

2       59. In addition, by failing to immediately notify all affected Uber Users that their  
3 personal information had been acquired or may have been acquired by unauthorized persons  
4 in the data breach, Defendants violated Civil Code § 1798.82. Defendants' failure to  
5 immediately notify Uber Users of the breach caused Class Members to suffer damages  
6 because they have lost the opportunity to immediately: (i) buy identity protection, monitoring,  
7 and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the  
8 theft of their Social Security numbers to financial institutions, credit agencies, and the Internal  
9 Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit,  
10 financial, utility, explanation of benefits, and other account statements on a monthly basis for  
11 unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or  
12 medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely  
13 monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and  
14 other forms of criminal, financial and medical identity theft, and repair damage to credit and  
15 other financial accounts; and (viii) take other steps to protect themselves and recover from  
16 identity theft and fraud.

17       60. Because they violated Civil Code § 1798.81.5 and 1798.82, Defendants "may  
18 be enjoined" under Civil Code § 1798.84(e).

19       61. Plaintiffs request that the Court enter an injunction requiring Defendants to  
20 implement and maintain reasonable security procedures to protect its employees' personal  
21 information, including, but not limited to, ordering that Defendants:

- 22               (a) engage third party security auditors/penetration testers as well as internal  
23               security personnel to conduct testing consistent with prudent industry  
24               practices, including simulated attacks, penetration tests, and audits on  
25               Defendants' systems on a periodic basis;
- 26               (b) engage third party security auditors and internal personnel to run automated  
27               security monitoring consistent with prudent industry practices;
- 28               (c) audit, test, and train its security personnel regarding any new or modified

- 1 procedures;
- 2 (d) purge, delete and destroy, in a secure manner, Uber Users data not
- 3 necessary for its business operations;
- 4 (e) conduct regular database scanning and securing checks consistent with
- 5 prudent industry practices;
- 6 (f) periodically conduct internal training and education to inform internal
- 7 security personnel how to identify and contain a breach when it occurs and
- 8 what to do in response to a breach consistent with prudent industry
- 9 practices;
- 10 (g) receive periodic compliance audits by a third party regarding the security of
- 11 the computer systems, cloud-based services, and application software
- 12 Defendants use to store the personal information of current and former Uber
- 13 Users;
- 14 (h) meaningfully educate its current and former Uber Users about the threats
- 15 they face as a result of the loss of their personal information to third parties,
- 16 as well as the steps they must take to protect themselves; and
- 17 (i) provide ongoing identity theft protection, monitoring, and recovery services
- 18 to Plaintiffs and Class Members, as well as their dependents and designated
- 19 beneficiaries of employment-related benefits through Defendants.

20 62. As a result of Defendants' violation of Cal. Civ. Code § 1798.81.5, Plaintiffs  
 21 and Class Members have incurred and will incur damages, including but not necessarily  
 22 limited to: (1) the loss of the opportunity to control how their personal information is used; (2)  
 23 the diminution in the value and/or use of their personal information entrusted to Defendants  
 24 for the purpose of deriving services from Defendants and with the understanding that  
 25 Defendants would safeguard their personal information against theft and not allow access and  
 26 misuse of their personal information by others; (3) the compromise, publication, and/or theft  
 27 of their personal information; (4) out-of-pocket costs associated with the prevention,  
 28 detection, and recovery from identity theft and/or unauthorized use of financial and medical

accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised personal information to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their personal information , which remain in Defendants' possession and are subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the personal information compromised as a result of the data breach for the remainder of the lives of the Class Members.

63. Plaintiffs seek all remedies available under Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including California Code of Civil Procedure § 1021.5

### **RELIEF REQUESTED**

64. Plaintiffs, on behalf of themselves, and all others similarly situated, request the Court enter judgment against Defendants, as follows:

- (a) An order certifying the proposed Class, designating Plaintiffs as named representatives of the Class, and designating the undersigned as Class Counsel;
- (a) An order enjoining Defendants from further unfair and deceptive business practices regarding the maintenance and protection of Uber Users' personal information;

- 1 (b) An award to Plaintiffs and the Class for compensatory, exemplary, and  
2 statutory damages, including interest, in an amount to be proven at trial;  
3 (c) A declaration that Defendants must disgorge, for the benefit of the  
4 Class, all or part of the ill-gotten revenues they collected from their  
5 conduct alleged herein, or make full restitution to Plaintiffs and Class  
6 Members;  
7 (d) An award of attorneys' fees and costs, as allowed by law;  
8 (e) An award of attorneys' fees and costs pursuant to California Code of  
9 Civil Procedure § 1021.5;  
10 (f) An award of pre-judgment and post-judgment interest, as provided by  
11 law; and  
12 (g) Such other relief as may be appropriate under the circumstances.

13 **DEMAND FOR JURY TRIAL**

14 65. Pursuant to Federal Rule of Civil Procedure 38(b) and Northern District of  
15 California Local Rule 3-6, Plaintiffs demand a trial by jury of any and all issues in this action  
16 so triable.

17 Dated: November 22, 2017

Respectfully submitted,

Capstone Law APC

20 By: /s/ Bevin Pike

21 Bevin Allen Pike  
22 Robert K. Friedl  
23 Trisha K. Monesi

24 Attorneys for Plaintiffs Susan Webber and Livia  
25 Soibelman  
26  
27  
28